Chinese Collection of U.S. Internet Traffic

U.S. ARMY

(U) This infographic provides insight on China-linked hackers breaching U.S. Internet Providers. A group of Chinese government-linked hackers, known as Salt Typhoon, have infiltrated multiple US telecommunications firms, potentially accessing sensitive information bearing on national security, including wiretap warrant requests. The breach was recently discovered and is being investigated by US officials, who are concerned about the potential national security damage. The Chinese government has denied the allegations and accused the US of politicizing cybersecurity issues.

Event:

- China-linked hackers have infiltrated U.S. internet providers
- Potentially accessed sensitive information and gained footholds in critical broadband networks
- Hackers specifically targeted network used by federal government for court-authorized wiretapping
- Attack is one of many Chinese-linked cyber attacks targeting major U.S. critical infrastructure and companies over the past several years.

Actors:

- A new group of Chinese government-linked hackers, known as "Salt Typhoon," infiltrated several U.S. Internet service providers (ISPs) and is believed to be attempting to steal sensitive information by accessing routers that control network traffic. This group has not been publicly identified until now.
- "Typhoon" is the code name given to a nation-state actor linked to the Chinese government, following a series of reports of cyber threats attributed to this group since the beginning of 2024. Other nation-state actors are also given names related to natural disasters and meteorological phenomena, such as "Blizzard" for Russia, "Sleet" for North Korea, and "Sandstorm" for Iran.

Impact:

- The hackers targeted a sensitive U.S. surveillance system used by the FBI and other agencies for court-authorized wiretapping in criminal and national security investigations. The system is maintained by several companies, and the hackers may have had access to the network infrastructure for several months.
- Recent Chinese-linked cyber attacks have been incredibly stealthy and sophisticated, similar to attacks attributed to Russia in the past. These attacks involve complex techniques allowing hackers to gain persistent access into networks, evade detection, and conceal their traffic.

Targeted Organizations:

AT&T

AT&T Inc., is an American multinational telecommunications holding company. It is the world's third largest telecommunications company by revenue and has 115.4 U.S. subscribers as of 31 Jun 2024.

LUMEN

Lumen Technologies, Inc. is an American telecommunications company, which offers communications, network services, security, cloud solutions, voice and managed services through its fiber optic and copper networks, as well as its data centers and cloud computing services

verizon

Verizon Communications Inc., is an American telecommunications company It is the world's second-largest telecommunications company by revenue and has 114.8 million U.S. Subscribers as of 31 Mar 2024

There is concern that the Chinese could potentially access various types of communications, such as text messages, internet traffic, and phone calls. Accessing and compromising these sensitive assets requires knowledge of the network structure and advanced capabilities to move across separate sub-networks. It is assumed that these assets are located far from the ISP corporate and operational network and are also connected to law enforcement networks to securely operate and stream gathered data.

- Sygnia Cybersecurity Services

Sources: The Chinese Hackers Spying on U.S. Internet Traffic (WSJ); China's Salt Typhoon Hacked AT&T, Verizon: Report (Security Week; Chinese government hacker 'Salt Typhoon' has infiltrated multiple internet providers (Gigazine); Salt Typhoon APT Subverts Law Enforcement Wiretapping: Report (Dark Reading)

Jeffrey T. Hardimon
CCoE G-2, Threat Branch